REMARKS

These remarks follow the order of the paragraphs of the office action. Relevant portions of the office action are shown indented and italicized.

DETAILED ACTION

Response to Amendment

In response, the applicants respectfully state that the exceptions to the cited art previously stated still stand.

Specification

> *The disclosure is objected to because of the following informalities:* on line 5 of the claim 1, "each the events" should be "said events" *Appropriate correction is required.*

In response, the applicants respectfully state that although it is believed that a claim amendment need not be reflected as a specification change, in order to be responsive, the specification is amended on line 5 of the claim 1, replacing "each the events" with "said each event."

Claim Objections

> *Claim 1 is objected to because of the following informalities: online 5 of the claim 1, "each the events" should be "said events".. Appropriate correction is required.*

In response, the applicants respectfully state that claim 1 is amended to 'said each event'. This overcomes the claim objection of claim 1.

Claim Rejections - 35 USC § 101

> *35 USC. 101 reads as follows:*
> *Whoever invents or discovers any new and useful process, machine manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.*
> *The base claim 1 recite a method of monitoring events in a computer network and the claim 10 recites "a computer program containing a program code to carry out the steps of the method of claim 1". Thus, the claim 1's method is a computer implemented method claim. The claim 1 recites steps in a computer program.*

> *Patentable subject matter is held to exclude laws of nature, natural phenomena, and* ***abstract ideas.*** *Diamond v. Liehr, 450 U.S 175, 185, 101 S.Ct 1048, 1056 (1981). Applicants' claim 1 recites steps in a computer program, which is not a process, and thus the claim 1 is non-statutory.*
>
> *Only an applicant's claims are entitled to the protection of the patent system; therefore claims, if expressing ideas in a mathematical form, must describe something beyond the manipulation of ideas in order to qualify as patentable subject matter. in re Warmerdam, at 1360. Given the absence of any practical effect or significant independent physical acts, the applicants' claim fails to adequately define the claimed invention within the domain of patentable subject matter The claimed invention as a whole must accomplish a practical application. That is, it must produce a "useful, concrete and* ***tangible result.****" State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. The purpose oft this requirement is to limit patent protection to inventions that possess a certain level of "real world" value, as opposed to subject matter that represents nothing more than art abstract idea or mathematical concept or is simply starting point for future investigation or research (Brenner v. Manson, 383 U.S. 519 528-36 148 USPQ 689, 693- 96); In re Ziegler, 992, F.2d 1197, 1200-03,26 USPQ2d 1600, 1603-06 (Fed. Cir. 1993)).*
>
> *Accordingly, a complete disclosure should contain some indication of the practical application for the claimed invention, i.e., why the applicant believes the claimed invention is useful. Given the absence of any practical effect or significant independent physical acts, the applicants' claim fails to adequately define the claimed invention within the domain of patentable subject matter.*
>
> *Claims 2-11, 16-17 are rejected for the same reason set forth in above.*

In response, the applicants respectfully state that claim 1 is not a computer implemented method claim. Claim 1 is a process having the particular steps indicated. There is nothing abstract about the steps of claim 1. Claim 1 includes tangible non-abstract ideas of a physical process. It includes at least one event trigger, event monitor, event display, display labels, event plots, viewer, event visualizer, etc.

Dependent claim 10 is a limitation upon independent claim 1. It does not reflect upon its parent claim negatively. If any problem exists it is with claim 10 not claim 1. Claim 10 let us say, is for claim differentiation of method claim 1. As a matter of fact the principle of claim differentiation makes claim 10 show that not all steps of claim 1 are computer implemented, otherwise claim 10 would not be necessary. Claim 10 includes components any of which can be implemented with tangible physical media. Claim 10 is amended to better show that it is a way to implement all the steps of claim 1 using a computer readable program. This overcomes the claim objection of claim 1.

> *The claim 11 recite "said program code being stored on data carrier". It is suggested that the preamble be amended to recite - said program code being stored on a computer readable medium."*

In response, the applicants respectfully state that claim 11 is amended to show that the program code is stored on a computer readable medium. This overcomes the claim rejection of claim 11.

> *The claim 13 recites . "a computer usable medium". It is suggested that the preamble be amended to recite - a computer readable medium."*

In response, the applicants respectfully state that claim 13 is amended to show that the program code is stored on a computer readable medium. This overcomes the claim rejection of claim 13.

> *The claim 14 recites "a program storage device readable by machine". It is suggested that the preamble be amended to recite - a computer readable medium."*

In response, the applicants respectfully state that claim 14 is amended to show that it is readable by a computer. This overcomes the claim rejection of claim 14.

> *The claim 15 recites "a computer usable medium". It is suggested that the preamble be amended to recite - a computer readable medium."*

In response, the applicants respectfully state that claim 15 is amended to recite - a computer readable medium. This overcomes the claim rejection of claim 15.

Claim Rejections - 35 USC § 112

> *The following is a quotation of the second paragraph of 35 U.S.C. 112: The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.*
>
> *Claims 1-20 are rejected under 35 USC. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.*
>
> *For example, the claim 1 recites "attribute values allocated to a given set of attributes of said each event", "various event attributes", "a primary attribute of the events", "a second display label to the events indicating the attribute values of the attributes'. "'a secondary attribute of said each event". It is confusing whether the attributes as recited ire the claim 1 are associated with a plurality of events or a single event. It is further confusing whether the attribute values as recited in the claim 1 are associated with a*

plurality of attributes or a single attribute such as a primary attribute or a secondary attribute. Clarification is required.

Although multiple attribute values related to the primary attribute can be presented on the same display, it is not ascertained that the attribute values are allocated to a plurality of attributes or to a single primary attribute as applicant's claim 1 later recites "a secondary attribute".

Moreover it is not ascertained from the claim invention set forth in the claim 1 whether the claim limitation of "attributes" refer to numerical attributes or categorical attributes or the display coloring attributes. Applicant flailed to particularly point out and distinctly claim the subject matter which applicant regards as invention.

Claims 2-13 and 15-19 depend upon the claim 1 and are rejected due to their dependency on the claim 1.

In response, the applicants respectfully state that it was shown above that claim 1 is amended to show that each event has a set of attributes. As stated in claim 1, each event has "a given set of attributes." As further stated attributes have "attribute values allocated to a given set of attributes of said each event. Claim 1 is amended to make it more clear and definite. The word 'attributes' is used as defined in the specification, Page 1, lines 13-19 which read:

"Network activities are usually monitored by the intrusion detection system as a time-ordered sequence of events wherein each event is characterized by a given set of attributes, so-called dimensions. Each event therefore forms an n-dimensional space."

"The monitoring of a high number of events each having many attributes triggered by an intrusion-detection system is a task that requires high skill and attention from the monitoring staff, since a large fraction of the triggered events is regularly reported.

Each event having a set of attributes. This overcomes the rejection under 35 USC. 112, second paragraph, of claim 1 and *Claims 2-13 and 15-19* which depend on claim 1.

The claim 14 is subject to the same rationale of rejection set forth in the claim 1.

In response, the applicants respectfully state that claim 14 is amended as in claim 1. This overcomes the rejection under 35 USC. 112, second paragraph, of claim 14.

The claim 20 is subject to the same rationale of rejection set forth in the claim 1.

In response, the applicants respectfully state ha claim 14 is amended as in claim 1. This overcomes the rejection under 35 USC. 112, second paragraph, of claim 20.

> *Claim 10 recites the limitation "the steps" in line 1 of the claim. There is insufficient antecedent basis for this limitation in the claim.*

In response, the applicants respectfully state that claim 10 is amended to overcome the rejection under 35 USC. 112, second paragraph.

> *Claim 11 recites the limitation "the steps" in line 1 of the claim. There is insufficient antecedent basis for this limitation in the claim.*

In response, the applicants respectfully state that claim 11 is amended to overcome the rejection under 35 USC. 112, second paragraph.

> *Claim 12 recites the limitation "the steps" in line 2 of the claim and the device" in lines 1-2 of the claim. There is insufficient antecedent basis for this limitation in the claim.*

In response, the applicants respectfully state that claim 12 is amended to overcome the rejection under 35 USC. 112, second paragraph.

> *Claim 13 recites the limitation "the steps" in line 4 of the claim. There is insufficient antecedent basis for this limitation in the claim.*

In response, the applicants respectfully state that claim 13 is amended to overcome the rejection under 35 USC. 112, second paragraph.

> *Claim 15 recites the limitation "the functions" in lines 4-5 of the claim. There is insufficient antecedent basis for this limitation in the claim.*

In response, the applicants respectfully state that claim 15 is amended to overcome the rejection under 35 USC. 112, second paragraph.

> *Claim 20 recites the limitation the method" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim.*

The scope of claim 20 is confusing as it is unclear whether an apparatus (i.e., an article of manufacture) or a method (i.e., a method) is being claimed. Clarification is required.

In response, the applicants respectfully state that claim 15, for an article of manufacture is amended to overcome the rejection under 35 USC. 112, second paragraph.

Claim Rejections -35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have bean obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention is made.

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over S. Ma, et al., "EventMiner: An integrated mining tool for Scalable Analysis of Event Data", May 21, 2001, www.research.ibm.com in view of D. Kranzlmuller, S. Gradbner, T. Volkert, ***"Event graph visualization for debugging large applications", Proc. of the SIGMETRICS symposium on Parallel mid distributed tools,*** *Philadelphia, PA, United States, Pages: 108 - 117 (hereinafter Kranzlmuller).*

In response, the applicants respectfully state that Claims 1-20 are apparently not made obvious by the combined art references to S. Ma, et al., and Kranzlmuller. Applicants respectfully state that continued exception is taken with the so called equivalencies of elements in Claims 1-20 and the cited art, as stated previously. This is particularly in regard to use of words in claims 1-20 of 'attributes', 'primary', 'events', 'display label' etc. Further exception is taken with the so called equivalencies of elements in Claims 1-20 and the combined art. The present invention, claimed in Claims 1-20, is for:

"Monitoring events triggered by a computer network. Each event being provided with attribute values allocated to a given set of attributes, and providing an event display, determining a primary attribute and a corresponding display label of the events selected from the given set of attributes presented with attribute values on a cross plot, providing a pattern algorithm to detect whether an arrived event is part of a given pattern, providing a mapping algorithm to map attribute values on the cross plot, allocating a second display

> label to the events indicating the attributes uncovered as part of the given pattern, plotting events arriving and including an attribute value allocated to a primary attribute into the cross plot, and plotting events arriving within the time period and detected by the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern."

The cited document of S. Ma, et al, Dated: May 21, 2001, is entitled: "EventMiner: An integrated mining tool for Scalable Analysis of Event Data". The Ma abstract reads :

> "Exploring large data sets typically involves activities that interwoven the following: querying databases, mining the results returned, and visualizing both the raw data and the parterres discovered. This interweaving of functions arises both from the semantics of what the analyst hopes to achieve and from salability requirements for dealing with large data volumes. Herein is described a tool, EventMiner, that integrates querying mining , and visualization so as to better analyze temporal data. We discuss the novel visualization techniques employed such as visualizing the results of data mining. Also, we address the large scale visualization of categorical data and how intelligent ordering of data can aid in this task. Though out, we illustrate the capabilities of EventMiner by applying it to event data from large computer networks.

Thus Ma is concerned with mapping events that have been queries from a database along the temporal axis, i.e. In the order in which they were presumably received, or recorded. Ma recognizes that time is only one possible visualization axis however does not offer any alternatives, nor gives indication of the potential use or usefullness of any other axis. Ma is primarily concerned with abstracting data from large volume to abstract visual representations.

Ma is not concerned with visualizing data that are being received from sensors directly, i.e. without intermediate storage in a database, and, even more importantly, is not concerned with visualizing the data along primary or secondary attribute axis, as in claims 1-20. In this present patent we believe the value of the visualization does not come from the abstraction that Ma offers, but by automatically generating a large variety of visualizations along many different attribute axis, and identifying correlations etc., by superimposing and cross-referencing these visualizations as in claims 1-20.

The other cited document of D. Kranzlmuller, S. Gradbner, J. Volkert, is entitled: "Eventgraph visualization for debugging large applications". The Kranzlmuller abstract reads :

> "Software repair and performance tuning of parallel programs are two difficult tasks in the parallel software lifecycle. The difficulties are further increased, if the target system is a parallel machine executing a program with many processes on a large amount of data. The existing debugging tools attack this problem with different approaches concerning monitoring and visualization techniques. The event graph visualization or space-time diagram is only one possibility to perform the analysis, but it is included by many existing tools.
>
> An example for usage of the event graph is ATEMPT, A Tool for Event ManiPulaTion. The functionality for error debugging (errors in the communication structure, race conditions) and for performance analysis (bottlenecks through blocking communication) is bated on this global communication graph. Extensions to the regular visualization are the abstraction mechanisms provided by ATEMPT. Through horizontal end vertical abstraction the event graph can be used to debug even large applications. The key relies on reducing the visualized information of data that are important for error detection and performance tuning."

Thus Kranzlmuller is concerned with the abstraction of large data volumes into smaller sets that can be visualized effectively. Kranzlmuller is not concerned with generating a variety of views onto the data set, along different attribute axis, without abstraction or reduction, as in claims 1-20. There is apparently no reason to combine Ma with Kranzlmuller except in an attempt to find elements of claims 1-20 using hindsight. This is not allowed. Besides even the combination does not make claims 1-20 obvious.

Most particularly, besides the differences stated in previous responses, the combined art is not concerned with superimposing and cross-referencing different visualizations of the same data, as in claims 1-20. Combining Kranzlmuller with Ma does not overcome the argument made in previous responses and in this response. Thus claims 1-20 are allowable over the cited combined art.

> *Claim 1:*
>
> *Ma teaches a method of monitoring events in a computer network, the method comprising: Said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes of said each event (The term "attributes" are not clear as it may be related to the data object attributes for each event or the pattern attributes for each pattern for a plurality of data objects). However, the pattern attributes for a plurality of data objects are also related to the data object attributes as a pattern is computed from the plurality of data objects. The cited reference teach mapping a plurality of data attributes to item to identify correlation's across different hosts and event types by using the mapping that maps the pair of event type and host name to item and eaves key empty. See Page 11. Moreover the cited reference in Page 1, second paragraph, explicitly teaches the attribute values, see the last paragraph of Page 6 and the first and second paragraphs of Page 8, the last paragraph of Page 12, and the real data set collected from a production computer network containing thousands of managed nodes including routers, hubs and servers are described in the last paragraph of page 3 and identifying unknown event patterns that can be used for real-time monitoring is described in the second paragraph of page 3. Ma has also taught* ***a plurality of pattern attributes related to the one or more significant measurements such as the co-occurrences****, i.e., the total number of times that two hosts generate events within a predefined time window, the conditional probability of the two hosts, i.e., the probability of a host generating an event given the observation that the other host has generated an event, the chi-squared test and so on); Simultaneously monitoring various event attributes versus the arrival time of said events (e.g., Fig. 5(b) displays two different attributes for the events; Figs. 2 and 4 show y-axis is the host name attribute as well as the coloring of attributes such as "authentication failure" event in red and "SNMP request events in green; therefore, at least two event attributes such as host name, authentication failure, SNMP request have been simultaneously monitored in the plot of Figs. 2 and 4); Providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis present an attribute value range (e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. See Page 11. Figs. 2, 4, 6, 7, 9 and the third paragraph of Page 8 describes a scatter plot or cross plot having any-axis representing around 160 hosts of a communication network and the x axis has been described in the figures as well as the first paragraph of page 6; for attribute value range, see these figures as well as the description in the second paragraph of Page 8); Determining a primary attribute of the events selected from the given set of attributes to be presented with its attribute values on the y-axis of the cross plot (e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. The attributes including the categorical attributes or temporal attributes and the primary attribute*

values are displayed in Figs. 2, 4, 6 and 7 and multiple attributes are described in the last paragraphs of Page 11 and 12).

Allocating a first display label (e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs, 2, & 7 and 9 such as 'Link down of host A" and 'node down of host B") to the events (e.g., alarms in Page 10) indicating (mapping of the attributes wherein the mapping results are shown in the plots with the patterns identifying indicating the attribute values of the primary attribute related to the categorical attribute such as the host A or the host B. Moreover, the pattern attribute values identifying the pattern 1 and the pattern 2 also describe the primary attribute such as the host A and the host B for the patterns such as "Link down of host A" and "node down of host B") the attribute values of the primary attribute (e.g., co-occurrence of certain events or the categorical attribute and event type associated with the events wherein the primary attribute is related to the primary attribute of the data set or the primary attribute of the patterns, See Page 12 and the key attribute values are described in the second paragraph of page 3), providing a pattern algorithm (the pattern algorithm is described in Fig. 7 as well as the mining algorithm as described in the last paragraph of page 12 or the EventMiner for ordering categorical values wherein the event generating, say every 300 seconds, 'may be identified) to detect whether an arrived event (arrived event are the selected event objects or the selected data objects in specific time range related to the events progressively loaded from a database or the mining alarm logs in a real time system,' see first paragraph of page 13 and the last paragraph of page 10 and a new query that retrieves the relevant data objects for more analysis in which a new query is restricted to a range constraint for a numerical attribute; see the last paragraph of page 10) is part or the given pattern (is part of the given pattern such as the Pattern 1 or the Pattern 2 from the identifiable patterns such as the SNMP request, authentication failure, link up, link down, port up, port down, wherein authentication failure indicates a possible security intrusion and link down of host A indicates the attribute associated with the data objects as well as the attribute associated with the event) on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event (e.g., the co-occurrence measurements for events can be computed for the data sets or the data objects and the temporal correlation with the selected hosts from the other side of the Attribute Viewer can be identified using the color linkage by the coloring and filtering algorithm or the data mining algorithm in which the difference or similarity in terms of patterns indicated by colors is compared; see page 12-13), providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot (see the last paragraphs of Page 11-12; The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty.), Allocating a second display label (e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7; SNMP request, authentication failure, link up, link down port up, port down wherein authentication failure indicates a possible security intrusion may be used as display labels as well. The attribute values may be used as display labels as well) to the events indicating the attribute values of the attributes being uncovered (discovered) as part of *the given pattern (e.g. the co-occurrence measurements for events can be computed and the temporal correlation with the selected hosts from the other side of the Attribute Viewer can be identified using the color linkage by the coloring and filtering algorithm or the data mining algorithm in which the difference or similarity in terms of patterns indicated by colors is compared; see page 12-13; the display labels indicate the attribute values of the attributes being discovered as part of the given pattern, for example, the second host was near a critical level for a key metric indicates the attribute values of the attributes being discovered as part of the given pattern), plotting all the events arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position of the first display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time (e.g., The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. Figs. 2, 4, 6, and 7 and the related paragraphs mentioned above in "allocating a first display label ". e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7; SNMP request, authentication failure, link up, link down, port up, port down wherein authentication failure indicates a possible security intrusion may be used as display labels as well. The attribute values may be used as display labels as well), and Plotting the all events arrived within the time period (Figs. 2, 4, 6, and 7 plot the all events within a specific time range) and being detected by means of the pattern algorithm (by the event miner algorithm) as part of the given pattern into the cross plot with the second display label (e.g. one a/the colors indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or (he cross plot of Figs. 2, 6, 7 and 9 or Pattern 2 or the Green Spike in Fig. 10, the position of the second display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event (see Figs. 1-10) on the basis of the attribute value of the attribute of the event being uncovered (uncovered far example in the alarm log and uncovered by the mining algorithm) as pan of the given pattern and its arrival time (discovered as part of the given pattern such as Patterns 1-4 and its arrival time; all the selected events are in a specific time range as plotted in Figs. 2, 4, 6, 7 and 10).*

In other words, Ma discloses an apparatus and system for monitoring events in a computer network enabling an operator of an intrusion-detection system to simultaneously monitor various event attributes versus the arrival time of the events, for example, authentication failure indicates a possible security intrusion may be used as display labels. The cited prior art teaches in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute values indicating the troublesome hosts having significantly high event counts) versus time with the attribute values for events in a communication network and the primary attribute for a host is selected from a plurality of attributes related to the categorical values. the one or more significant measurements such as the co-occurrences (i.e., the total number of times that two hosts generate events within a predefined time window), the conditional probability of the two hosts (i.e., the probability of a host generating an event given the observation that the other host has generated an event), the chi-squared test and so on.

Fig. 4 shows the coloring of the events having the primary attribute with the patterns indicating the authentication failure and SNMP request in order to differentiate using the coloring the events with authentication failure from other events. A. pattern label is assigned to the events falling into the same pattern. Finally, the operator can view different event attributes by switching menus (Fig. 6).

Ma has taught in Fig. 7 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute values indicating the troublesome hosts having significantly high event counts) versus time with the attribute values for events in a communication network. Ma has also taught a plurality of attributes related to the one or more significant measurements such as the co-occurrences (i.e., the total number of times that two hosts generate events within a predefined time window), the conditional probability of the two hosts (i.e., the probability of a host generating an event given the observation that the other host has generated an event), the chi-squared test and so on wherein the attribute values are plotted in the same plot. See Figs. 2, 6, 7 and 9. Many significant event patterns are simultaneously identified within a single plot without the operator's switching between the various event attributes.

Ma discloses display label including the colors for coloring the different patterns that indicate the attribute values of the primary attribute such as the co-occurrences of some specific events within a predefined time window.

Ma teaches in Fig. .5(b) displays two different attributes for the events; Figs. 2 and 4 show y-axis is the host name attribute as well as the coloring of attribute such as "authentication failure" events in red and "SNMP request events in green,- therefore at least two event attributes such as host name authentication failure, , SNMP request have been simultaneously monitored in the plot of Figs. 2 and 4. The menu options shown in Fig. 6 allow for the y-axis attribute mappings be changed. Moreover, Ma teaches mapping a plurality of attributes to item and viewing both numerical attribute and categorical attribute on a same plot in Fig. 7 (See Page 10). Thus, Ma at least teaches or suggests the claim limitation of viewing a secondary attribute of said each event together with the primary attribute on said display.

Moreover, Kranzlmuller teaches viewing a plurality of attributes P0-P7 for the events in a communication network. Kranzlmuller teaches viewing a secondary categorical attribute (e.g., an event belonging to the category P0) of said each event together with the primary categorical attribute (e.g., an event belonging to the category P1) on said display (See Page 109 Fig. 2).

It would have been obvious to one of the ordinary skill in the art at the time the invention was made to have incorporated Kranzlmuller's teaching into Ma to view a plurality of attributes related to the events on the same display because Ma at least suggests the claim limitation of viewing a secondary attribute of said each event together with the primary attribute on said display at least by the means of mapping of the secondary attribute and coloring the secondary attribute and therefore the secondary attribute arid the primary attribute are distinctly viewed (See Figs. 2 and 4 of Ma wherein a plurality of secondary attributes are colored so as to be viewed. Although the menu options are used in Figs. 6 of Ma to switch the primary attribute to the another attribute, the secondary attribute can be viewed by the coloring mechanism as disclosed and can be further queried and displayed in different slots on the same display).

> _ *One of the ordinary skill in the art would have been motivated to do so such that the inter-process dependency among events and event categorical attributes are visualized (Kranzlmuller Page 109).*

In response, the applicants respectfully state that the combined art of Ma and Kranzlmuller apparently do not make claim 1 obvious. Claim 1 as amended reads:

1. A method of monitoring events in a computer network, the method comprising:

said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes of said each event,

simultaneously monitoring various event attributes from said given set of attributes versus the arrival time of said each event,

providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis presenting an attribute value range, and visualizing data along said x and y coordinate axes, said axes being attribute axes,

determining a primary attribute of said each event selected from the given set of attributes to be presented with its attribute values on the y-axis of the cross plot,

allocating a first display label to the events indicating the attribute values of the primary attribute, providing a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,

allocating a second display label to said each event indicating the attribute values of the attributes being uncovered as part of the given pattern, plotting all events that arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position of the first display label of said each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time,

plotting all events that arrived within the time period and being detected by means of the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern, the position of the second display label of said each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the given pattern and its arrival time,

viewing a secondary attribute of said each event together with the primary attribute on said display; and

automatically generating a large variety of visualizations along other attribute axes, and identifying correlations by superimposing and cross-referencing these visualizations.

The applicant respectfully take particular exception with the alleged equivalency of elements in claim 1 and the cited art, and take exception with the Examiner assertions. For example, claim 1 shows that the attribute are event attributes, and to show explicitly that it includes "simultaneously monitoring various event attributes versus the arrival time of each the events," and to specifically add a step of "viewing a secondary attribute of said each event together with the primary attribute on said display." This apparently more clearly distinguishes claim 1 from the cited reference. Thus claim 1 and all claims that depend thereupon are allowable over Ma.

Claim 1- 20 state that the value of the visualization is derived from generating multiple visualizations along different attributes and using those to identify interesting event patterns by superposition and cross-referencing.

A review of Ma and Kranzlmuller show that even the combination does not steps of claim 1. The combination does not do the steps of automatic generation of multiple visualizations and providing means for cross-referencing. Thus the combined art does not make claim 1 obvious, and claim 1 and all claims depending on claim 1 are allowable.

> *Re Claims 2-3: Ma further discloses selecting the new events within the specified time period and plotting the new events within the shifted time period into the cross plot. See Figs. 6, 7, 9 and 10 in which events in the two time periods are drawn and the spikes are identified and the newly selected events are redrawn as determined by the data mining algorithm for the time period during which the new events are retrieved. The database records the attribute values and the arrival time of a new event. The pattern algorithm determines on the basis of the recorded attribute values of event whether or not the newly arrived event in the database and the newly retrieved event from the database includes an attribute value of the primary attribute for a certain host and event type, as determined the pattern algorithm using the mapping mechanism for mapping a plurality of attributes including the primary attribute into an item for presentation, and the pattern algorithm also determines if the newly arrived event e.g., alarm, includes the attribute value for the primary attribute, e.g., a certain host or a certain event type including SNMP request, authentication failure link up, link down, port up, port down, link dawn of host A, node down of host B etc., shifting the x-axis of the cross plot for the new time period so that the new time period being presented on the x-axis covers the arrival time of the event and plotting the event arrived within the shifted time period into the cross plot with the first display label indicating the primary attribute.*
>
> *Ma discloses determining on the basis of the recorded attribute values of event from the alarm log or the database whether or not the newly arrived event for the new time period is part of the given pattern using the pattern algorithm on the basis of a comparison of the attributes allocated to the given pattern, for example a composite pattern of Page 13, on the basis of a comparison analysis, and of the attribute assigned to the arrived event wherein the newly arrived event are determined by the retrieval time ranges and data ranges including the host names and types from the database. Ma further discloses determining if the newly arrived event includes an attribute value of the given pattern including the mutual dependence measurement of an m-pattern adding the event to the previous events being detected as part of the given pattern, and redrawing all the events being associated with given pattern in the cross plot by updating the cross plot.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claims 2 and 3 and the cited art, and take exception with the Examiner assertions. This is in regard to use of words in the claims attributes, primary, events, display label etc. The present invention in 2 and 3 is not anticipated or made obvious by S. Ma, et al. As noted Ma's method is apparently that only one of the event attributes may be plotted versus the arrival time of the events. Thus, the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event attribute or attributes or their simultaneous display. Ma is not concerned with the 'primary attribute' nor for a plurality of event attributes, as in claims 2 and 3. The addition of Kranzlmuller apparently does nothing to make these obvious.

Also, the office communication states the visualizations are generated for any type of attribute, or combination of several, recorded with the event data. A review of Ma and Kranzlmuller show that the art still is concerned with data along a temporal axis. Thus, claims 2 and 3 are allowable over Ma and Kranzlmuller in themselves and because each depends on allowable claim 1.

> *Re Claims 4-5: Ma further discloses the third display label and the fourth display label indicating the new patterns (See the three colored spikes in Fig. 6 and the four patterns in Fig. 7).*
>
> *Ma discloses determining if the newly arrived event does not include an attribute value of the given pattern, on the basis of the recorded attribute values of all previous arrived events from the alarm logs or from the database, by means oft the mining algorithm whether or not the newly arrived event is part of a new pattern on the basis of a comparison (Page 13) of the attribues allocated to the new pattern and of the attributes assigned to the arrived events. Ma discloses allocating a third display label to the events, including the coloring of the new pattern, indicating the attribute values of the attributes being discovered as part of the new pattern wherein a large amount of patterns can be discovered by the mining algorithms. Ma discloses plotting the all events being detected by means of the mining algorithm as part of the new pattern into the cross ploi with the third display label indicating the new pattern the position of the third display label of each event in the cross plot being determined by the mapping algorithm (Page 12 for the mapping of the attributes into item and thereby determining the positions of the patterns on the cross plot) on the basis of the attribute value of the attribute of the event (event types, host names etc.) being uncovered as part of the new pattern, such as SNMP request authentication failure, link up, Link down, port up, pore down, link down of host A, node down of host B etc., and its arrival time in the database.*
>
> *Ma discloses removing all the events including an attribute value allocated to the primary attribute from the cross plot, if a primary attribute to be presented with its attribue values on the y-axis of the cross plot is changed (if the mapping mechanism for mapping a plurality of attributes including the host names and event types are changed), allocaing a fourth display label including SNMP request, authentication fai we, link up, link down, port up, port down, link dawn of host A, node dawn of host B etc., to the events indicating the attribute values of the new primary attribute (e.g., category attribute, event type of data objects). Ma discloses plotting all the events arrived within the time period as retrieved from the database and including an aitribute value allocated to the new primary attribute into the cross plot with the fourth display label, including SNMP request, authentication failure, link up, link down, port up, port down, link down of host 4, node down of host B etc., indicating the new primary attribute, such as the host name and event type, the position of the fourth display label of each event in the cross*

plot being determined by the mapping mechanism in Page 12 on the basis of the attribute value of the primary attribute of the event and its arrival time as determined by the retrieval condition from the database.

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claims 4 and 5 and the cited art, and take exception with the Examiner assertions. This is in regard to use of words in the claims attributes, primary, events, display label etc. The present invention in 4 and 5 is not anticipated or made obvious by S. Ma, et al. As noted, applicants respectfully state that the indicating of new patterns in Ma, is not the steps of claim 4. Ma and Kranzlmuller do not test as in claim 4, "if the newly arrived event does not include an attribute value of the given pattern " Nor do Ma and Kranzlmuller determine, "on the basis of the recorded attribute values of all previous arrived events by means of the pattern algorithm whether or not the newly arrived event is part of a new pattern on the basis of a comparison of the attributes allocated to the new pattern and of the attributes assigned to the arrived events." Nor do Ma and Kranzlmuller test, "if the newly arrived event forms together with previous recorded events the new pattern," Nor do Ma and Kranzlmuller allocate, "a third display label to the events indicating the attribute values of the attributes being uncovered as part of the new pattern." Certainly, Ma and Kranzlmuller does apparently not perform the step of, "plotting the all events being detected by means of the pattern algorithm as part of the new pattern into the cross plot with the third display label indicating the new pattern, the position of the third display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the new pattern and its arrival time.

Similarly, Ma with or without Kranzlmuller are not concerned with a 'primary attribute nor with the step of claim 5, of <u>removing all the events including an attribute value allocated to the primary attribute from the cross plot,</u> if a primary attribute to be presented with its attribute values on the y-axis of the cross plot is changed, allocating a fourth display label to the events indicating the attribute values of the new primary attribute," nor with the step of, "plotting all the events arrived within the time period and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label indicating the new primary attribute, the position of the fourth display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time," nor with the step of, "if a primary attribute to be presented with its attribute values on the y-axis of the cross plot is changed, allocating a fourth display label to the events indicating the attribute values of the new primary attribute, and plotting all the events arrived within the time period and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label indicating the new primary attribute, the position of the fourth display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time.

Also, for example, the office communication states "the application of data mining algorithms, which are then used to generated multiple different visualizations. A review of Ma and Kranzlmuller show that even the combination does not equal that generation of multiple visualizations for cross-referencing. Thus claims 4 and 5 are allowable over Ma and Kranzlmuller in themselves and because each depends on allowable claim 1.

> *Re Claim 6: Ma further discloses the operator selects the events to be plotted and displaying textual and coloring information associated with the selected events on the event display (Page 4 and Figs. 6,7, 9-10).*
>
> *Ma discloses plotting all attribute values, including the attributes such as event type, link down, and host name, host A, in the patterns marked as the link down of host A, node down of host B, recorded for an event, as retrieved from the database, with the respective display label into the cross plot if the event is selected by an operator and displaying textual information associated with the selected event on the event display.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 6 and the cited art, and take exception with the Examiner assertions.

In response, applicants respectfully state that exception is taken with the so called equivalencies of elements in Claim 6 and the cited art. This is in regard to use of words in the claims attributes, primary, events, display label etc. The present invention in claim 6 is not anticipated by S. Ma, et al. As noted, applicants respectfully state that Ma is not concerned with the test and step of claim 6 of, "plotting all attribute values recorded for an event with the respective display label into the cross plot if the event is selected by an operator, and displaying textual information associated with the selected event on the event display.

Also, a review of Ma and Kranzlmuller show that the user has to guide the visualization manually. Thus claim 6 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Re Claim 7: Ma further discloses a pattern algorithm such as the data mining algorithm suitable to perform multi-attribute pattern recognition (Figs. 6, 7, 9-10).*
> *Ma discloses the mining algorithm being suitable to perform multi-attribute pattern recognition using the mapping mechanism (Page 12) and the pattern comparisons matching (Page 13).*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 7 and the cited art, and take exception with the Examiner assertions. The present invention in claim 7 is not anticipated by S. Ma. There is apparently no indication that Ma is concerned with multi-attribute pattern recognition or even any pattern recognition as in claim 7. Being allegedly suitable is indeed not an anticipation of the invention in claim 7. Thus claim 7 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Re Claim 8: Ma further discloses using color such as Red and Green to color the pattern Spikes and Pattern 1, Pattern 2, Pattern 3, Pattern 4 for specific mark layouts (Figs. 6, 7, 9-10).*
> *Ma discloses each display label includes different colors marking the events.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 8 and the cited art, and take exception with the Examiner assertions. A review of Ma and Kranzlmuller show that even the combination does not have the elements as in claim 8. Thus, claim 8 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Re Claim 9: Ma further discloses all events being uncovered as part of the pattern being clustered by the display label such as Red Spikes, Green Spikes (Figs. 6, 7 and 9-10).*
> *Ma discloses all events being discovered as part of the pattern as clustered by the different labels including Red Spikes and Green Spikes to indicate one of the plurality of events such as SNMP request, authentication failure link up, link down, port up, port down, link down of host A, node down of host B etc., indicating the new primary attribute.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 9 and the cited art, and take exception with the Examiner assertions. There is apparently no indication that Ma is at all concerned with clusters or clustering as in claim 9. Thus claim 9 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Re Claim 10: Ma further discloses a data mining algorithm and GUI (Page 14). Ma discloses the mining algorithm carrying the steps as recited in the claim 1.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 10 and the cited art, and take exception with the Examiner assertions. The response to claim 1 is appropriate to claim 10 which depends thereupon. The program code is that of claim 1, which is not anticipated by Ma. Claim 10 is amended. Thus claim 10 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Re Claim 11: Ma further discloses the program code being stored on data carrier (see page 5). Data cattier is inherent within the computer embodiment of Page 5.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 11 and the cited art, and take exception with the Examiner assertions. Exception is taken with the stated inherentcy. There is apparently no indication that Ma or Kranzlmuller discloses or is concerned with a data carrier as in claim 11. Thus claim 11 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Re Claim 12: Ma further discloses an event visualization device for monitoring events in a computer network (Page 3). The cited reference teach mapping a plurality of data attributes to item to identify correlations across different hosts and event types by using the mapping that maps the pair of event type and host name to item and leaves key empty. See Page 11. Moreover, the cited reference in Page 1, second paragraph, explicitly teaches the attribute values, see the last paragraph of Page 6 and the first and second paragraphs of Page 8, the last paragraph of Page 12 and the real data set collected from a production computer network containing thousands of managed nodes including routers, hubs and servers are described in the last paragraph of page 3 and identifying unknown event patterns that can be used for real-time monitoring is described in the second paragraph of page 3.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 12 and the cited art, and take exception with the Examiner assertions. The present invention in claim 12 is not anticipated by S. Ma. The response to claim 1 is appropriate to claim 12, which depends thereupon. The device is for performing the steps of claim 1, which is not anticipated by Ma. Thus claim 12 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Re Claims 13 and 15: Ma further discloses an implementation of the Event Miner algorithm, on the computer (Page 4-5).*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claims 13 and 15 and the cited art, and take exception with the Examiner assertions. In response, applicants respectfully state that exception is taken with the so called equivalencies of elements in Claims 13-16 and the cited art. The present invention in claim 13-15 are not anticipated by S. Ma. The response to claim 1 is appropriate to claim 13 and 15, which depends thereupon. Claim 14 is amended to be an independent claim of the Beauregard type, with all the elements of claim 1. The implementations are for performing the steps of claim 1, which is not anticipated by Ma. Thus claims 13-15 are allowable over Ma and Kranzlmuller for itself and because it depends on, or has the matter, of allowable claim 1.

> *Claim 14: The claim 14 is subject to the same rationale of rejection set forth in the claim 1.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 14 and the cited art, and take exception with the Examiner assertions. Claim 14 is amended as in claim 1. The response to claim 1 is appropriate to amended claim 14. Thus claim 14 is allowable over the combined art of Kranzlmuller and Ma.

> *Claim 16: The claim 16 is subject to the same rationale of rejection set forth in the claims 2 4.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 16 and the cited art, and take exception with the Examiner assertions. There is apparently no indication that Ma and Kranzlmuller perform the added steps of claim 16. The present invention in claim 16 is not anticipated by S. Ma. The response to claim 1 is appropriate to claim 16, which depends thereupon. The method is for performing more steps over the steps of claim 1, which is not anticipated by Ma. Thus claim 16 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Claim 17: The claim 17 is subject to the same rationale of rejection set forth in the claim 5.*

In response, applicants respectfully state that as with claim 5 exception is taken with the so called equivalencies of elements in Claim 17 and the cited art. This is in regard to use of words in the claims attributes, primary, events, display label etc. There is apparently no indication that Ma and Kranzlmuller perform the added steps of claim 17. The present invention in claim 17 is not anticipated by S. Ma. The response to claim 1 is appropriate to claim 17, which depends thereupon. The method is for performing more steps over the steps of claim 16, which is not anticipated by Ma. Thus claim 17 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Claim 18: The claim 18 is subject to the same rationale of rejection set forth in the claims 2-4.*

In response, applicants respectfully state that as with claims 2-4, exception is taken with the so called equivalencies of elements in Claim 18 and the cited art. This is in regard to use of words in the claims attributes, primary, events, display label etc. There is apparently no indication that Ma and Kranzlmuller has the added elements of claim 18. The present invention in claim 18 is not anticipated by S. Ma. The response to claim 1 is appropriate to claim 18, which depends thereupon. The device is for more elements than claim 5, which is not anticipated by Ma. Thus claim 18 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Claim 19: The claim 19 is subject to the same rationale of rejection set forth in the claim 5.*

In response, applicants respectfully state that as with claim 5 exception is taken with the so called equivalencies of elements in Claim 19 and the cited art. This is in regard to use of words in the claims attributes, primary, events, display label etc. There is apparently no indication that Ma and Kranzlmuller perform the added steps of claim 19 has the added elements of claim 189. The response to claim 1 is appropriate to claim 17, which depends thereupon. The device is for more elements than claim 5, which is not anticipated by Ma. Thus claim 17 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

> *Claim 20: The claim 20 is subject to the same rationale of rejection set forth in the claim 1.*

In response, the applicant respectfully take particular exception with the alleged equivalency of elements in claim 20 and the cited art, and take exception with the Examiner assertions. As with claim 1, claim 20 shows that the attribute are event attributes, and to show explicitly that it includes "means for simultaneously monitoring various event attributes versus the arrival time of each the events," and to specifically include "means for viewing a secondary attribute of said each event together with the primary attribute on said display." This apparently more clearly distinguishes claim 1 and 20, from the cited reference. Thus claim 20 is allowable over Ma and Kranzlmuller.

It is anticipated that this amendment brings the application to allowance of claims 1-20. Favorable action is respectfully solicited. In the unlikely event that any claim remains rejected, please contact the undersigned as required by the MPEP, by phone in order to discuss the application.

Please charge any other fee necessary to enter this paper to deposit account 50-0510.

Respectfully submitted,

By: /Louis Herzberg/
Dr. Louis P. Herzberg
Reg. No. 41,500

Voice Tel. (845) 352-3194
Fax. (845) 352-3194

3 Cloverdale Lane
Monsey, NY 10952

Customer Number: 54856